Available online at http://www.ijasrd.org/in

International Journal of Advanced Scientific Research & Development

Vol. 03, Iss. 01, Ver. II, Jan – Mar' 2016, pp. 134 – 139

e-ISSN: 2395-6089
p-ISSN: 2394-8906

AN EFFICIENT CLOUD SECURITY SYSTEM USING DOUBLE SECRET KEY DECRYPTION PROCESS FOR SECURE CLOUD ENVIRONMENTS

A. Maheswari[1]

R. Sanjana[1]

S. Sowmiya[1]

[1] Final Year Students, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

Sudhir Shenai[2]

G. Prabhakaran[2]

[2] Assistant Professor, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

ARTICLE INFO

Article History:

Received: 08 Mar 2016;
Received in revised form:
13 Mar 2016;
Accepted: 13 Mar 2016;
Published online: 31 Mar 2016.

Key words:

Privacy Preserving,
Key Revocation,
Security Encryption,
Access Control Policy

ABSTRACT

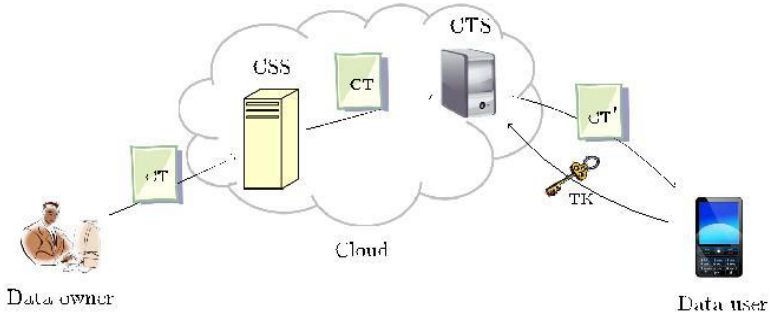
Internet technology is growing quickly, and people can process, store, or share with their data by using its ability. Cloud shares infrastructure between several organizations and it is managed internally or by a third-party. The user stores the data in an encrypted format. ABE is an encryption scheme used by the user to store the data in the cloud. ABE is a public-key based one to many encryption techniques which allows users to encrypt and decrypt data based on user attributes. Access control of encrypted data stored in the cloud is, by using access polices and ascribed attributes associated with private keys and cipher texts. In existing ABE schemes decryption has expensive paring operations and the complexity of the access policy is proportional to the number of attributes. An ABE system with outsourced decryption eliminates the decryption overhead. Here user provides data to the cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied with the user's attributes or access policy into a simple cipher text. In this paper, use the security model of ABE with verifiable outsourced decryption by providing the verification key at the time of output decryption. We can implement this approach in real time cloud environments.

How to cite this article: Maheswari, A., Sanjana, R., Sowmiya, S., Shenai, S., & Prabhakaran, G., (2016). "An Efficient Cloud Security System Using Double Secret Key Decryption Process for Secure Cloud Environments". *International Journal of Advanced Scientific Research & Development (IJASRD), 03* (01/II), pp. 134 – 139.

INTRODUCTION

Cloud security design is efficient only if the right defensive implementations are in place. Efficient cloud protection architecture should know the issues that will arise with security management. The security management tackles these issues with security controls. Various access control forms are in use, including the most common User Access Control (UAC), Attribute Access Control (AAC) and Role Based Access Control (RBAC). All these models are known as character based access control models. In all these access control models, consumer (subjects) and resources (objects) are identified by unique names. Identification may be done straight or through roles assigned to the subjects. These access control techniques are effective in unchangeable distributed system, where there are only a set of consumers with a known set of services. Users are usually identified by their attributes or characteristics and not by predefined characteristics. In such cases, the conventional identity based access control models are not very much efficient and therefore, contact to the system must be done on decision based on convinced attributes. In addition, in the cloud system, self-directed domains have a separate set of security policies. Hence, the access control machine must be bendable to support various kinds of domains and policies. With the progress of large distributed systems attribute based access control (ABAC) has happen to increasingly important.

Fig.1: *System Model for ABE with Outsourced Decryption*



RELATED WORK

B Waters[3] proposed a new methodology for realizing Cipher text-Policy ABE systems from a general set of access structures in the standard model under concrete and non-interactive assumptions. They can be implemented both decisional-Bilinear Diffe-Hellman Exponent (d-BDHE) and decisional-Bilinear Diffie-Hellman assumptions and presented the first cipher text-policy attribute-based encryption systems that are efficient, expressive, and provably secure under concrete assumptions.

A Goyal[5] analyze the semi-functional keys and cipher texts are not used in the real system, only in the proof of security. The proof employs a hybrid argument over a sequence of security games. The first is the real security game, with normal keys and cipher text. In the second game, the cipher text is semi-functional and the keys remain normal. In subsequent games, the keys requested by the attacker are changed to be semi-functional one by one. By the final game, none of the keys given out are actually useful for decrypting a semi-functional cipher text, and proving security becomes relatively easy.

Bethencourt[7] is able to prove the ability to do something in an examination and then get the corresponding credential, without presenting any identifying information.

Alternatively, one might interact with a service via a pseudonym (e.g. a login name) and wish to obtain attributes relating to this interaction without revealing one's full identity.

V. Goyal & A. Jain[4] presents the first construction of a cipher text-policy attribute based encryption scheme having a security proof based on a number theoretic assumption and supporting advanced access structures. Previous CP-ABE systems could either support only very limited access structures or had a proof of security only in the generic group model. Our construction can support access structures which can be represented by a bounded size access tree with threshold gates as its nodes.

PRIVACY – PRESERVING AUTHENTICATION PROTOCOL

Security and privacy are very vital issues in cloud computing. In existing system access control in clouds are central in nature. The scheme uses a symmetric key approach and does not hold authentication. Symmetric key algorithm employs same key for both encryption and decryption. The authors get a centralized approach where a sole key distribution center (KDC) distributes secret keys and attributes to all consumers. In existing system, address the aforesaid privacy issue to suggest a shared authority based privacy preserving authentication protocol (SAPA) for the cloud storage, which realize authentication and authorization lacking compromising a user's personal information. This system classify a new privacy challenge in cloud storage, and address a restrained privacy issue during a user demanding the cloud server for data sharing, in which the challenged request itself cannot disclose the user's privacy no matter whether or not it can obtain the contact authority. Propose an authentication protocol to augment a user's access demand related privacy, and the shared access authority is achieved by anonymous access demand matching mechanism. Apply cipher text-policy attribute based access control to appreciate that a user can reliably access its possess data fields, and adopt the proxy re-encryption to supply temp authorized data sharing among multiple users. The existing process preserve implement new approach that is shared authority approach to supports anonymous authentication. The user is genuine using multifactor approach includes biometric authentication. The proposed format is resilient to replay attacks. In this scheme using Elliptic Curve Diffie Hellman (ECDH) for authentication purpose, ECDH is the one of several cryptographic algorithms, most often used to verify that a file has been unaltered. And also implement attribute based access control whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, environment attribute etc.). Implement this process in real time cloud environments and improve accuracy of the system.

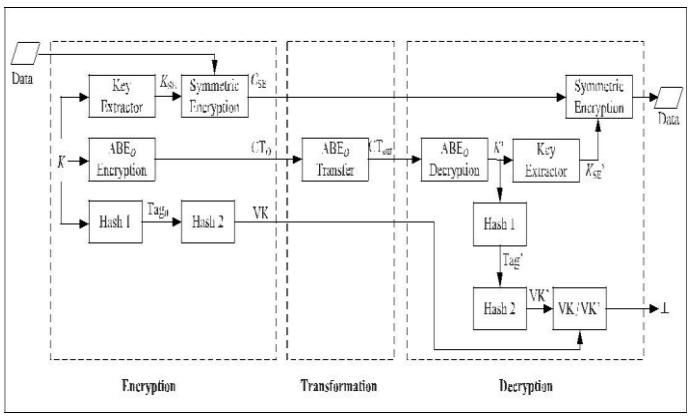


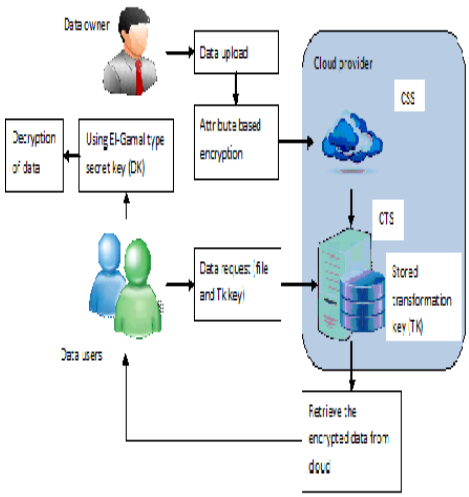
Fig 2: The framework of generic construction of verifiable outsourced ABE.

PROPOSED METHODOLOGY

4.1 Attributed Based Key Encryptions Problem:

The Cloud storage is an important service of cloud computing. The Cloud Storage offers services for data owners to host their data into the cloud. Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Moreover, while updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys. To solve the privacy issue on shared data, propose an OPOR framework for Secure Data Sharing in Public Clouds proposed merkle hash tree. This algorithm presents a feasible replacement for traditional public key cryptosystem that requires trusted third party to issue key to bind user to their public keys .TTP generates its own signature on each user public keys and manage user keys, thus overall key management in this system is way too expensive and complex. The newly proposed system uses access control mechanism. In Access control policy is employed to encrypt each data to solve the key escrow problem. In this algorithm user first provide its ID to the cloud which returns private key to the user in interim also item to the owner of plain text then encrypt the data using the public key and transmit the encrypted data along the public keys to the cloud and the user downloads and decrypt the data. If the user revoke from group means, can change the public key to entire groups.

Fig. 3: *Access Control Mechanism*



EXPERIMENTAL RESULTS

In this chapter evaluate the performance of the system using the performance metrics such as storage overhead, communication cost and computation efficiency. The storage overhead is one of the most significant issues of the access control scheme in cloud storage systems. In this scheme, besides the storage of attributes, each shared authority id also needs to store a public key and a secret key for each user in the system.

Thus, the storage overhead on each shared authority in this scheme is also linear to the number of in the system. The communication cost of the normal access control is almost

the same. The communication cost of attribute revocation is linear to the number of cipher texts which contain the revoked attribute. Compare the computation efficiency of both encryption and decryption in two criteria: the number of authorities and the number of attributes per authority.

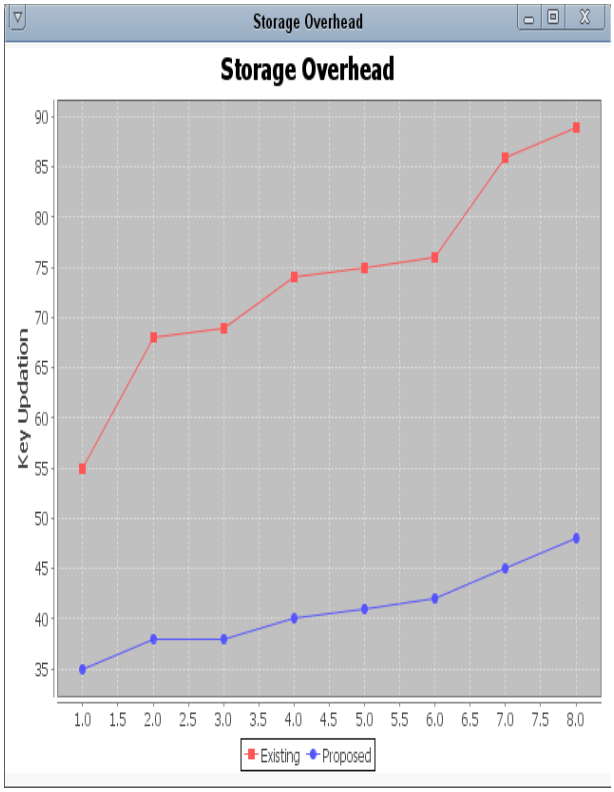


Fig 4: Storage Overhead performance

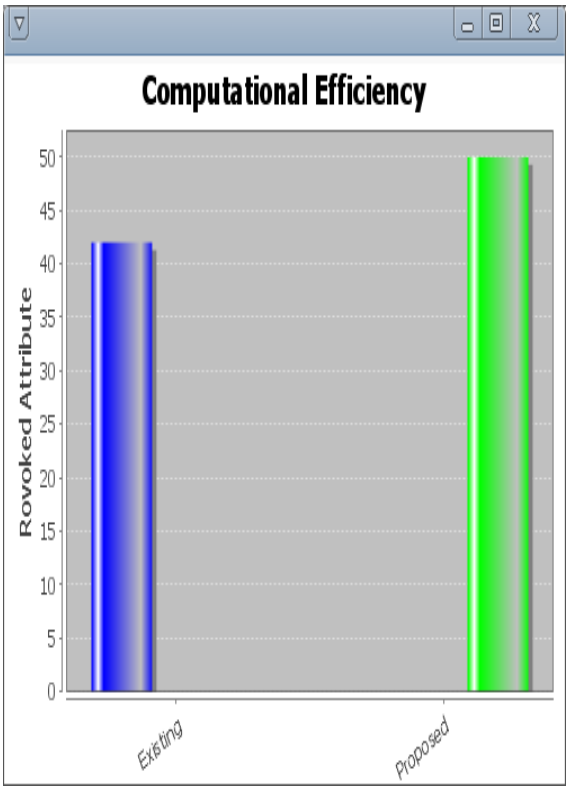


Fig 5 Computational Efficiency

CONCLUSION

This paper proposes a novel framework of achieving grained access control for sharing personal data. Considering partially trustworthy cloud servers, it argues that to fully realize the concept, patients shall have complete control of their own privacy through encrypting their files to allow fine-grained access. The framework addresses the unique challenges brought by multiple data owners and users, in that greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. It utilizes ABE to encrypt the cloud data, so that user can allow access not only by personal users, but also various users from public Data owner mains with different professional roles, qualifications, and affiliations. Considered a new requirement of ABE with outsourced decryption: Verifiability. It is used to modify the original model of ABE with outsourced Decryption. This ABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .This scheme does not rely on random oracles. A flexible access control for encrypted data stored in cloud is provided. It eliminates Decryption overhead for user according to attributes.This Data transformation is guaranteed to store in cloud. This secure attribute based cryptographic technique for robust data security that's being shared in the cloud. Furthermore enhance attribute scheme to multi authority attribute scheme to handle efficient and on demand user revocation, and

prove its security. As future study, it will be interesting to enhance the fine grained access control in cloud computing with authorized CTS to verify the cloud server that stores and process the cloud records.

REFERENCES

[1] A. Sahai & B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, & B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, & B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.

[5] Y. Rouselakis & B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Secur., 2013, pp. 463–474.

[6] L. Cheung & C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 456–465.

[7] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, & C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," Theoretical Comput. Sci., vol. 422, pp. 15–38, Mar. 2012.

[8] M. Green, S. Hohenberger, & B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Secur. Symp., 2011, p. 34.

[9] J. Lai, R. H. Deng, C. Guan, & J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[10] R. Gennaro, C. Gentry, & B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 465–482.